Linear Algebra and its Applications 484 (2015) 46–62

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

An asymptotic formula for the number of irreducible transformation shift registers

Stephen D. Cohen [a], Sartaj Ul Hasan [b], Daniel Panario [c,*], Qiang Wang [c]

[a] *School of Mathematics and Statistics, University of Glasgow, Glasgow G12 8QW, Scotland, United Kingdom*
[b] *Scientific Analysis Group, Defence Research and Development Organisation, Metcalfe House, Delhi 110054, India*
[c] *School of Mathematics and Statistics, Carleton University, Ottawa, K1S 5B6, Canada*

ARTICLE INFO

Article history:
Received 22 February 2014
Accepted 15 June 2015
Available online 2 July 2015
Submitted by R. Brualdi

MSC:
15B33
12E20
11T71
12E05

Keywords:
Block companion matrix
Characteristic polynomial
Irreducible polynomial
Primitive polynomial
Galois group
Transformation shift register

ABSTRACT

We consider the problem of enumerating irreducible transformation shift registers. We give an asymptotic formula for the number of irreducible transformation shift registers in some special cases. Moreover, we derive a short proof for the exact number of irreducible transformation shift registers of order two using a recent generalization of a theorem of Carlitz.

* Corresponding author.
E-mail addresses: Stephen.Cohen@glasgow.ac.uk (S.D. Cohen), sartajulhasan@gmail.com (S.U. Hasan), daniel@math.carleton.ca (D. Panario), wang@math.carleton.ca (Q. Wang).

http://dx.doi.org/10.1016/j.laa.2015.06.020
0024-3795/

1. Introduction

Linear feedback shift registers (LFSRs) are devices that are used to generate sequences over a finite field. This sort of sequence has received numerous applications in various disciplines including in the design of stream ciphers; see, for example, [12,15]. For all practical purposes, these sequences are generally considered over a binary field. The sequences with maximal period have been proved to have good cryptographic properties. LFSRs corresponding to sequences with maximum period are known as primitive LFSRs.

The number of primitive LFSRs of order n over a finite field $\mathbb{F}_q$ is given by

$$\frac{\phi(q^n-1)}{n}, \tag{1}$$

where ϕ is Euler's totient function. A similar formula for the number of irreducible LFSRs (that is, when the characteristic polynomial of the LFSR is irreducible) of order n over a finite field $\mathbb{F}_q$ is given by

$$\frac{1}{n}\sum_{d|n}\mu(d)q^{\frac{n}{d}}, \tag{2}$$

where μ is the Möbius function.

Niederreiter [16] introduces the notion of *multiple recursive matrix method*, which may be considered as a generalization of the classical LFSRs. Zeng et al. [21] consider the notion of σ-LFSR which is a word-oriented stream cipher. It turns out that the latter is essentially same as Niederreiter's multiple recursive matrix method. A conjectural formula for the number of primitive σ-LFSRs of order n was given in the binary case in [21]. An extension of this conjectural formula over the finite field $\mathbb{F}_{q^m}$ given in [10] states that this number is

$$\frac{\phi(q^{mn}-1)}{mn}q^{m(m-1)(n-1)}\prod_{i=1}^{m-1}(q^m-q^i). \tag{3}$$

We refer to [10] and [11] for recent progress on this conjecture and to [4] for a proof of this conjecture.

It is also known from [11] and [4], see also [18], that the number of irreducible σ-LFSRs is

$$\frac{1}{mn}q^{m(m-1)(n-1)}\prod_{i=1}^{m-1}(q^m-q^i)\sum_{d|mn}\mu(d)q^{\frac{mn}{d}}. \tag{4}$$

We focus on *transformation shift registers* (TSRs) in this paper. This notion was introduced by Tsaban and Vishne [20] and it can be also considered as a generalization of classical LFSRs. The notion of TSR was introduced to address a problem of Preneel